How to interpret remediation estimates

This page has been made public for vendors

Question

Where did the remediation estimates provided in secure code review validation reports come from - what are they for and how were they generated?

Answer

Approximate remediation estimates are provided to assist with planning remediation work, if or as might be appropriate. Note that some bugs are harder to fix than others. Modifying a single line of code in a self-contained method is easier than modifying the result of a sequence of calls that span the application. Systems development program and project-specific considerations should also be taken into account.

Remediation estimates come from predefined values (remediation effort values) stored in HPE Fortify SCA software rulepacks. When a scan is performed using HPE Fortify SCA, the remediation effort value is saved as part of the information stored for each finding reported in the scan file (FPR). Individual rules contain remediation effort values that are defined by HPE. HPE Fortify defines the term *remediation effort* as the relative amount of effort required to fix and verify a finding.

Benefits of using the HPE Fortify SCA provided remediation effort values to determine the remediation estimates are:

- Estimates specific to programming language and vulnerability type
- Organizational benefits realized by continuing to utilize and leverage the VA's investment in HPE Fortify SCA
- Best practices of leveraging the tools' built-in security knowledge, providing industry knowledge and consistency

Remediation effort values may be updated by HPE as new rulepacks are released, reflecting further refinement and enhancement of HPE Fortify SCA security knowledge over time. Remediation effort values are ranges of numbers, similar to agile story points, and indicate relative levels of effort.

Before remediation estimates are provided, the remediation effort values are first totaled, then converted into hours by multiplying by a representative VA-defined hour per point constant, and then adjusted to include VA-specific considerations. For example, issues concerning the way scans were conducted that violate the VA Secure Code Review SOP are calculated using VA-defined remediation effort values.

For issues not audited by the developer, default remediation effort values are used to reflect the estimated time needed to audit the findings, instead of the estimated time needed to fix the type of findings not audited. For additional findings identified and reported by the VA Software Assurance Program Office during validations (findings not reported by Fortify), default remediation effort values are used.

Fortify-defined remediation effort values for findings reported in a scan can be displayed from within Audit Workbench if desired. See **How to View Remediation Effort for Findings in Audit Workbench**

References

- HPE Security Fortify Audit Workbench User Guide, section "Estimating Impact and Likelihood with Input from Rules and Analysis"
- VA Secure Code Review SOP

HPE Fortify Version	16.20 and later
Programming Language	☑ C/C++ ☑ .NET ☑ Java ☑ Objective-C ☑ Other
Fortify Audit Workbench	☐ Yes ☑ No
Fortify IDE Plugin	☐ Yes ☑ No
Other Fortify Component	☑ Yes ☐ No

Request code review tools, validations, and support HERE.